REMARKS

In response to the Office Action dated February 10, 2005, Applicant respectfully requests reconsideration and withdrawal of the rejections of the claims.

Claim 1 was rejected under the second paragraph of 35 U.S.C. § 112. The Examiner questioned the role that is played by the function $\lambda(n)$. In the original translation of claim 1, two alternatives were presented for the formation of the private key. In one implementation of the invention, the private key is formed from the parameters p and q. In an alternative implementation, the private key is formed from the parameters p, q and $\lambda(n)$. In the previous amendment to claim 1, the alternative phrase was removed, as a result of which the claim positively recites on by the first implementation. Thus, as amended, the function $\lambda(n)$ does not play any role in the claimed method. Accordingly, the recitation of this function has been removed from claim 1, and is now presented in new claim 21. The Examiner is thanked for his observation on this point.

In the rejection of claim 1, the Examiner also questioned the role of the variable n, and suggested that the notation be changed to read $\lambda(p,q)$. It is respectfully submitted, however, that the original notation is consistent with the disclosure. As defined in claim 1, n is the product of p and q. As set forth in the application at page 7, lines 26-27, $\lambda(a)$ designates the Euler indicator of a. If $a=p.q$, $\lambda(a)=\text{LCM}(p-1,q-1)$. Accordingly, it is respectfully submitted that, when the claim is read in light the disclosure, one of ordinary skill in the art can understand the subject matter being claimed.

The rejection states that the variable m is not defined in claim 1. The definition of this variable appeared in claim 2, and that subject matter has now been incorporated into claim 1.

Claim 1 was rejected under 35 U.S.C. § 101, on the grounds that the claim fails to provide a tangible output. The tangible outputs resulting from the claimed method are public and private keys for cryptography. The formation of these keys is set forth in the last clause of claim, and therefore it is respectfully submitted that the claim complies with the requirements of 35 U.S.C. § 101. To advance the prosecution of the application, however, claim 1 has been amended to more explicitly recite the generation of the keys as positive steps of the claimed method.

Claims 2-20 were rejected under 35 U.S.C. § 101 on the grounds that they present claims directed to a system, but depend from method claim 1. The rejection states that "claims 2-20 may not be directed towards more than one statutory class of invention under the rules set forth under 35 U.S.C. § 101." It is respectfully submitted that claims 2-20 are not directed to more than one statutory class of invention. In particular, they are directed to a cryptographic communication system, which falls within the statutory class of "machine." The fact that some of the components of this system, namely the public and private keys, are defined according to the manner in which they are generated does not violate the requirements of 35 U.S.C. § 101. Rather, this aspect of the claim is analogous to a product-by-process claim, which has been found to be an acceptable form of claim.

It is respectfully submitted that the currently pending claims comply with the requirements of 35 U.S.C. §§ 101 and 112. Since there has been no rejection of the claims on the basis of prior art, it is respectfully submitted that the application is in condition for allowance.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: May 10, 2005

By:
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620